The Great Debate

A military response to cyberattacks is preposterous

JUN 2, 2011 12:03 EDT

By Benjamin H. Friedman and Christopher Preble

The opinions expressed are their own.

According to the *Wall Street Journal*, the Pentagon's first cyber security strategy will say that cyberattacks can be acts of war meriting retaliatory military attack. The policy threatens to repeat the overreaction and needless conflict that plagued American foreign policy in the past decade. It builds on national hysteria about threats to cybersecurity, the latest bogeyman to justify our bloated national security state. A wiser approach would put the threat in context to calm public fears and avoid threats that diminish future flexibility.

A key challenge in responding to "cyberattacks" is defining that term. Reporters sometimes use it to describe hackers stealing credit card numbers or intellectual property. Website vandalism and denial-of-service attacks, where attackers flood websites with requests to overburden and disable them, are often included. Electronic espionage, including the theft of intellectual property or state secrets, also qualifies. More obvious kinds of cyberattack include attacks on military communication systems and hacking that sabotages infrastructure like electricity grids, water systems, or online banking.

The idea of responding militarily to most of these threats is preposterous. We thwart hackers with better passwords, IT professionals and policing, not aircraft carriers. We do not threaten to bomb countries caught spying on us in traditional ways and should not do so just because the prefix "cyber" applies.

The Pentagon will reportedly avoid this definitional difficulty with a policy of "equivalence," where only cyberattacks creating destruction on par with traditional military attacks qualify as acts of war. The trouble is that some acts of war, like naval blockades, damage only commerce. The same goes for all reported cyberattacks. Launching a war to retaliate for a non-lethal attack seems disproportionate, especially where it is unclear whether the attacker served the government. Taken literally, the new policy might have us risking nuclear exchange with Russia because it failed to stop teenagers in Moscow Internet cafés from attacking Citibank.com.

The real obstacle to making sensible cybersecurity policy is hysteria, which drowns out common sense. Cyberattacks have never killed an American, yet Senator Carl Levin compared them to

weapons of mass destruction. His colleague Jay Rockefeller said they "can shut this country down." Mike McConnell, the former director of national intelligence, called cyberattacks on financial systems "the equivalent of today's nuclear weapon."

These claims rely on the assertions of authorities like White House official-turned-security-consultant Richard Clarke. In a book that *Wired* reviewed under the title "File Under Fiction," Clarke and a co-author suggest that hackers could plunge our nation into chaos in minutes by shutting off power, crashing planes, flooding dams and shutting down stock trading. They obscure the fact that managers of that infrastructure prevent such catastrophes by decoupling it from the public Internet and having backup systems. Clarke ignores evidence showing that hackers have never caused a power outage, and that people rarely panic and loot when the lights go out.

We exaggerate online threats for the same reason we exaggerate other security threats: our information about the danger comes largely from those that benefit from the provision of defenses against it.

The media will print almost any claim about cyberwar, which combines two of its favorite subjects: disaster and the Internet. Pundits and ambitious officials know that doomsday predictions about the next big thing bring attention, promotions and contracting gigs. There is less reward in noting that the Internet heightens economic resilience by making it easier to replace suppliers and distributing information critical to most enterprises.

The $10 billion-plus that the federal government will spend this year on IT security creates a chorus of alarm among contractors and the communities where they park jobs. And agencies involved in cybersecurity — the National Security Agency, the Department of Homeland Security and the Pentagon's Strategic Command, for starters — justify their budgets with cyberalarm.

Competition for power also contributes to the problem. Agencies compete to own cybersecurity policy, as do the Congressional committees that oversee them. Several dozen cybersecurity bills now sit before Congress. Each request for authority, funds or legislative action comes with a claim that inaction leaves us vulnerable.

Cyberfears are not altogether phony. The Internet makes it harder to keep information private, facilitating crimes. Managing the problem requires a mix of liability, regulatory and law enforcement reforms, mostly in state capitals. The federal government has a role to play in securing its networks and secrets, pursuing hackers abroad, reporting on them and developing offensive hacking capabilities. The Stuxnet virus that afflicted Iran's nuclear program demonstrates that U.S. intelligence agencies and those of our allies' are the leading practitioners of cybersabotage. We should keep it that way.

Foreign powers know that killing Americans, whatever the means, will bring retaliation. Reminding them is sensible, but threatening war given vague hypotheticals may simply encourage belligerent decisions in the future. Rather than exaggerate our vulnerabilities, public officials should herald our

resilience, noting that most cyberattacks create hassle, not catastrophe, and that our ability to swiftly recover from even the worst attacks is our best defense.

Benjamin H. Friedman is a research fellow in defense and homeland security studies, and Christopher Preble is director of foreign policy studies, at the Cato Institute.
